



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/579,810	05/26/2000	Victor Kouznetsov	002.0132.01	7703

22895 7590 01/12/2004

PATRICK J S INOUE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER

WU, ALLEN S

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 01/12/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/579,810

Applicant(s)

KOUZNETSOV, VICTOR

Examiner

Allen S. Wu

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 May 2001.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 May 2000 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ 6) ☐ Other: _____

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "11" has been used to designate both system for dynamically detecting computer viruses through associative behavioral analysis and of runtime state and a client system. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
3. Claims 1, 7-9, 14-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
4. Claim 1 recites the limitation "which each" in line 4 of claim. There is insufficient antecedent basis for this limitation in the claim. Claims 9 and 17 also recite similar limitations
5. Claim 1 recites the limitation "the sequence" in line 10 of claim. There is insufficient antecedent basis for this limitation in the claim. Claims 9 and 17 also recite similar limitations

6. Claim 1 recites the limitation "the execution" in line 10 of claim. There is insufficient antecedent basis for this limitation in the claim. Claims 9 and 17 also recite similar limitations
7. Claim 6 recites the limitation "the class of actions" in line 2 of claim. There is insufficient antecedent basis for this limitation in the claim. Claim 14 also recites similar limitations.
8. Claim 7 recites the limitation "the group" in line 2 of claim. There is insufficient antecedent basis for this limitation in the claim. Claim 15 also recites similar limitations.
9. Claim 8 recites the limitation "the computer virus" in line 1 of claim. There is insufficient antecedent basis for this limitation in the claim. Claim 15 also recites similar limitations.
10. Claim 8 recites the limitation "the group" in line 2. There is insufficient antecedent basis for this limitation in the claim. Claim 15 also recites similar limitations.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 1, 5-9, 13-17, and 21 rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al, US Patent 6,088,804, in view of Nachenberg, US Patent 6,357,008.

As per claims 1, 9, and 17, Hill et al discloses dynamically detecting computer viruses through associative behavioral analysis of runtime state (abstract), comprising: defining a group of monitored events which each comprise a set of one or more actions defined within an object (security events, col 7 ln 55-67 and col 8 ln 1-3), each action being performed by one or more applications executing within a defined computing environment (nodes, col 7 ln 55-67 and col 8 ln 1-3); continuously monitoring the runtime state within the defined computing environment for an occurrence of any one of the monitored events in the group (continually respond, col 7 ln 55-67 and col 8 ln 1-3); tracking the sequence of the execution of the monitored events for each of the applications (first attack... number of security events, col 8 ln 22-35); identifying each occurrence of a specific event sequence characteristic of computer virus behavior (comparing task, col 8 ln 30-49); creating a histogram describing the specific event sequence occurrence for each of the applications (training signature into display map (col 7 ln 28-45); and identifying repetitions of the histogram associated with at least one object (comparing task, col 8 ln 30-49; also col 9 ln 8-25).

Hill et al further discloses identifying the location of a virus attack. However, Hill et al does not explicitly teach identifying the application, which

performed the specific event sequence. Nachenberg discloses a detection of infected programs, which identifies the application that performed the specific event sequence (target program, col 2 ln 39-45 and col 10 ln 11-53). One of ordinary skill in the art at the time of the applicant's invention would have been able to identify the application performing the specific event sequence in addition to the identification of the location of the virus. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Nachenberg within the teachings of Hill et al because it would have simplified the correction step through the extra knowledge of which application would possibly be infected.

In further regards to claim 1, Hill et al discloses a parameter set stored on a client system defining a group of monitored events (security agents...located at nodes, col 4 ln 30-41) and a monitor executing on the client system (identify security events, col 4 ln 19-41) comprising a collector continuously monitoring the runtime state within the defined computing environment for an occurrence of any one of the monitored events in the group (col 4 ln 30-41; also task 82 col 7 ln 54-67 and col 8 ln 1-3). Hill et al further discloses an analyzer (col 8 ln 5-29).

However, Hill et al does not teach the monitor comprising the analyzer.

Nachenberg et al discloses a monitor comprising a collector (decryption phase, col 7 ln 30-67 and col 8 ln 1-47) and an analyzer (col 8 ln 48-53 and col 9 ln 5-65). One of ordinary skill in the art at the time of the applicant's invention would have been able to combine the analyzer within the monitor executing on a client

system. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Nachenberg within the system of Hill et al because it would have improved efficiency by eliminating communication with a third party.

As per claims 5, 13, and 21, Hill et al further discloses detecting suspect activities within each histogram (compares, col 8 ln 30-49), each suspect activity comprising a set of known actions comprising a computer virus signature (training signature, col 7 ln 46-54 and col 8 ln 30-49).

As per claim 6 and 14, Hill et al discloses detecting viruses based on suspect activity (security events, abstract) being selected from a class of message transmissions (FTP requests, col 5 ln 45-65). However, Hill et al does not explicitly teach each suspect activity being selected from the class of actions comprising file accesses, program executions, configuration area accesses, security setting accesses, and impersonations. Nachenberg discloses monitoring suspect activity being selected from the class comprising file accesses, program executions, configuration area accesses, security setting accesses, and impersonations (col 9 ln 27-65). Activities are events that can be monitored as a security event. One of ordinary skill at the time of the applicant's invention would have been able to additionally monitor activities from the class of file accesses, program executions, message transmissions, configuration area

accesses, security setting accesses, and impersonations. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Nachenberg within the system of Hill et al because it would have improved security through a more robust list of activities to be monitored.

As per claims 7 and 15, Hill et al discloses detecting viruses based on suspect activity (security events, abstract). However, Hill et al does not explicitly teach each suspect activity being selected from a group comprising file accesses, program executions, direct disk accesses, media formatting operations, sending of electronic mail, system configuration area accesses, changes to security settings, impersonations, and system calls having the ability to monitor system input/output activities. Nachenberg discloses monitoring suspect activity being selected from the class comprising file accesses, program executions, message transmissions, configuration area accesses, security setting accesses, and impersonations (col 9 ln 27-65). Activities are events that can be monitored as a security event. One of ordinary skill at the time of the applicant's invention would have been able to additionally monitor activities from the class of file accesses, program executions, message transmissions, configuration area accesses, security setting accesses, and impersonations. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Nachenberg within the system

of Hill et al because it would have improved security through a more robust list of activities to be monitored.

Furthermore, the combination of Hill et al and Nachenberg does not teach the suspect activity being chosen from a group consisting of sending of electronic mail and system calls having the ability to monitor system input/output activities. The office takes official notice that activity relating to sending of email or system input/output activities is well known in the art. It would have been obvious to one of ordinary skill at the time of the applicant's invention would have been able to additionally monitor activities from the group of sending electronic mail and system calls having the ability to monitor system input/output activities in the combination of Hill et al and Nachenberg because it would have improved security through a more robust list of activities to be monitored.

As per claims 8 and 16, Hill et al further discloses monitoring computer viruses comprising at least one form of unauthorized content selected from the group comprising a computer virus application, a Trojan horse application, and a hoax application (col 5 ln 46-65).

13. Claims 2-4 and 10-12 and 18-20 rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al, US Patent 6,088,804, in view of Nachenberg, US Patent 6,357,008 as applied to claims 9 and 17 above, and further in view of Vaidya, US Patent 6,279,113

As per claims 2, 10, and 18, Hill et al discloses organizing the histograms into plurality of records (fig 3; col 5 ln 26-65; and col 7 ln 27-54) ordered by object and monitored event (fig 3). The combination of Hill et al and Nachenberg does not teach the records ordered by application. Vaidya discloses a system for detecting network intrusion (abstract) including a storage manager (database handler, col 5 ln 46-67) organizing a database of records ordered by application (network objects, col 5 ln 45-66 and col 6 ln 1-56). One of ordinary skill in the art at the time of the applicant's invention would have been able to order the database records by the application for which the record pertains to. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Vaidya within the combination of Hill et al and Nachenberg because it would have increased efficiency of the virus detection by allowing the detection to be specific to the application.

As per claims 3, 11, and 19, Hill et al further discloses maintaining a structured database in which the plurality of records is stored (col 5 ln 39-45); and storing a histogram for each such specific event sequence occurrence in one such database record (col 5 ln 39-45 and col 7 ln 27-45). The combination of Hill et al and Nachenberg does not teach storing the records identified by the application by which the specific event sequence was performed. Vaidya discloses a system for detecting network intrusion (abstract) including using a database of records ordered by application (network objects, col 5 ln 45-66 and

col 6 ln 1-56). One of ordinary skill in the art at the time of the applicant's invention would have been able to order the database records by the application for which the record pertains to. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Vaidya within the combination of Hill et al and Nachenberg because it would have increased efficiency of the virus detection by allowing the detection to be specific to the application.

As per claims 4, 12, and 20, Hill et al further discloses configuring the structured database as an event log organized by each event in the group of monitored events (fig 3, security events and frequency, col 8 ln 30-50); and updating the database record storing each specific event sequence occurrence with a revised histogram as each such occurrence is identified (Security system is adapted, col 9 ln 34-45).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Wells, US Patent 6,338,141 discloses a method and system for detecting viruses in real time.

Masaoka, Japanese Patent 08044556A, discloses protecting a computer from infectious programs.

Chambers, US Patent 5,398,196, discloses a method and system for detecting viruses through behavioral analysis.

Schnerrer, US Patent 5,842,002, discloses a method and system for detecting viruses through behavioral analysis.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-0900.

Allen S. Wu
Examiner
Art Unit 2135

ASW


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100